In the Claims:

This listing of claims will replace all prior versions, and listings of claims in the application. The status of each claim is indicated. Currently amended claims are shown with additions underlined and deletions in ~~strikethrough text~~. Claims 5, 8-20, and 32-34 have been previously cancelled. Please add new claims 46-51. No new matter has been added.

1.   (Currently Amended) A system for ensuring the identity and travel privileges of potential travelers, comprising:

a. at least one institution for researching and recording an identity and at least one travel privilege for individuals;

b. at least one database maintained by the institution for associating identified individuals' names, an assigned asymmetric key pair, and the at least one travel privilege, said at least one travel privilege including:

i. at least one destination restriction;

ii. at least one date and time restriction;

iii. at least one mode of transportation restriction;

iv. at least one operator restriction; and

v. an expiration date for each at least one travel privilege;

c. at least one travel privilege certificate associated with the at least one travel privilege and further associated with an identified individual; and

d. at least one personal identification device including a means for authenticating at the personal identification device the identified individual based on a biometric, the personal identification device configured such that the biometric is not output from the personal identification device.

2.   (Original) The system described in claim 1, wherein the travel privilege certificate comprises:

a. a name field, comprising the identified individual's full name;

b. a date field, comprising a date when the identified individual is allowed to travel;

c. a time field, comprising a time when the identified individual is allowed to travel;

d. a mode of transportation field, comprising a list of the modes of transportation that the identified individual is allowed to employ;

e. a type of privilege field, comprising the type of privilege signified by the travel privilege certificate;

f. an issue date field, comprising the date when the travel privilege certificate is issued;

g. an expiration date field, comprising the date when the travel privilege certificate is no longer valid;

h. a unique serial number; and

i. a digital signature created by the issuer of the travel privilege certificate.

3.   (Original) The system described in claim 2 wherein the list of the modes of transportation includes at least one mode selected from the group consisting of a train, a bus, a car, an airplane and a ship.

4.   (Original) The system described in claim 2 wherein the type of privilege is selected from the group consisting of a reservation ticket, a boarding pass, a port-of-entry permission and a vehicle operator permission.

5.   (Canceled)

6.   (Previously Presented) The system described in claim 1 wherein the at least one personal identification device includes:

a. means for communicating, the means for communicating programmed to download at least one travel privilege certificate to said personal identification device, download a computing mechanism onto the personal identification device, download a

digital certificate and asymmetric key pair for the individual into the personal identification device and transmit at least one travel privilege certificate from said personal identification device;

      b. means for recording at least one notable event on said personal identification device;

      c. means for storing at least one travel privilege certificate on said personal identification device and at least one application audit log on said personal identification device.

7.   (Previously Presented) The system described in claim 6, wherein the at least one personal identification device includes:

      means for receiving the biometric of the identified individual prior to the identified individual being authenticated based on the biometric and prior to transmitting the travel privilege certificate.

8-20.   (Canceled)

21.   (Currently Amended) A processor-readable medium located at a personal identification device and storing instructions that when executed cause a processor to perform the following method:

      authenticating, at a personal identification device, a biometric input from a user based on a biometric template stored at the personal identification device and associated with the user without sending the biometric template from the personal identification device; and

      sending a request for a travel permission information from the personal identification device when the biometric input from the user is authenticated.

22.   (Previously Presented) The processor-readable medium of claim 21, the method further comprising:

receiving the biometric input from the user before authenticating the biometric input from the user, the biometric input being at least one of a fingerprint information of the user, a retinal information of the user and an image information of the user.

23. (Previously Presented) The processor-readable medium of claim 21, wherein the request includes a personal identity credential from the user, the personal identity credential excludes the biometric input from the user and the biometric template associated with the user.

24. (Previously Presented) The processor-readable medium of claim 21, the method further comprising:

sending an admission ticket information associated with the travel permission information when the biometric input from the user is authenticated at the personal identification device.

25. (Previously Presented) The processor-readable medium of claim 21, wherein the travel permission information is associated with an admission ticket of a travel provider.

26. (Previously Presented) The processor-readable medium of claim 21, wherein the travel permission information includes at least one of a time restriction, a mode of transportation restriction, a destination restriction, a date restriction, an operator restriction, and an expiration date restriction.

27. (Previously Presented) The processor-readable medium of claim 21, wherein the travel permission information is encrypted based on an asymmetric key pair associated with a travel governing authority.

28. (Previously Presented) The processor-readable medium of claim 21, the method further comprising:

enrolling the biometric template at an enrollment station before the authenticating the biometric input from the user.

29.   (Currently Amended) A processor-readable medium located at a processor device and storing instructions that when executed cause a processor to perform the following method:

receiving a request for a travel permission information from a personal identification device associated with a user, the request including an acknowledgement of an authentication of the biometric information of the user performed at the personal identification device, without the biometric information of the user being sent from the personal identification device, the authentication acknowledgement excluding biometric information; and

sending the travel permission information associated with the user based on the acknowledgementauthentication, the travel permission information being encrypted based on an asymmetric key pair.

30.   (Previously Presented) The processor-readable medium of claim 29, wherein the request includes a personal identity credential of the user excluding biometric information, the method further comprising:

producing the travel permission information based on the personal identity credential of the user; and

sending the travel permission information associated with the user based on the personal identity credential of the user.

31.   (Previously Presented) The processor-readable medium of claim 29, the method further comprising:

obtaining the travel permission information associated with the user from a database before sending the travel permission information, the database including at least one personal identity credential for each user from a plurality of users, each user from the plurality of users being associated with at least one travel permission information.

32-34. (Canceled)

35.   (Previously Presented) The processor-readable medium of claim 29, wherein the travel permission information is sent to the personal identification device of the user.

36.   (Previously Presented) The processor-readable medium of claim 29, the method further comprising:

receiving the travel permission information from an enrollment station before the sending the travel permission information.

37.   (Previously Presented) The processor-readable medium of claim 29, wherein the travel permission information includes at least one of a time restriction, a mode of transportation restriction, a destination restriction, a date restriction, an operator restriction, and an expiration date restriction.

38.   (Previously Presented) The processor-readable medium of claim 21, wherein the personal identification device is portable and is programmed to be used when being transported.

39.   (Currently Amended) The processor-readable medium of claim 21, ~~wherein the user is an operator of a vehicle,~~ the method further comprising:

sending <u>an acknowledgement of</u> an authentication of the biometric input <u>of</u> ~~from~~ the user based on the biometric template associated with the user, the ~~authentication~~ <u>acknowledgement</u> excluding the biometric input of the user and the biometric template associated with the user.

40.   (Previously Presented) The processor-readable medium of claim 29, wherein the personal identification device is portable.

41.   (Currently Amended) The processor-readable medium of claim 29, the method further comprising:

receiving from the personal identification device the travel permission information associated with <u>the</u> user substantially at a time of ignition of a vehicle <u>and not before the ignition of the vehicle</u>, the travel permission information excluding biometric information; and

receiving from the personal identification device the travel permission information associated with the user at least one time when the user is operating the vehicle, the travel permission information excluding biometric information.

42.   (Previously Presented) The processor-readable medium of claim 29, the method further comprising:

receiving the travel permission information from a travel-governing authority associated with enrollment of the biometric information to the personal identification device.

43.   (Currently Amended) The processor-readable medium of claim 21, wherein the user is an operator of a vehicle, <u>the biometric input of the operator is a first biometric input of the operator,</u> the method further comprising:

<u>receiving, at the personal identification device, the travel permission information;</u>

<u>authenticating, at the personal identification device, a second biometric input from the operator based on the biometric template stored at the personal identification device and associated with the operator; and</u>

inhibiting output of a signal <u>the travel permission information</u> to a kill switch <u>coupled to the vehicle when the second biometric input of the operator is not authentic</u> such that the kill switch disables operation of the vehicle when the biometric input of the operator is not authentic.

44. (Currently Amended) The processor-readable medium of claim 21, wherein the user is an operator of a vehicle, the biometric input of the operator is a first biometric input of the operator, the method further comprising:

the authenticating, at the personal identification device, the a second biometric input of the operator of the vehicle substantially at a time of ignition of the vehicle and not before the ignition of the vehicle; the method further comprising: and

authenticating, at the personal identification device, the a third biometric input of the operator of the vehicle at least one time when the vehicle is in operation.

45. (Currently Amended) The processor-readable medium of claim 29, wherein the user is an operator of a vehicle, the method further comprising:

sending the travel permission information associated with the operator to a kill switch operatively coupled to the vehicle when the travel permission information is received from the personal identification device; and

not sending the travel permission information associated with the operator to the kill switch when the travel permission information is not received from the personal identification device such that a kill switch disables operation of the vehicle.

46. (New) The processor-readable medium of claim 21, wherein the user is an operator of a vehicle, the method further comprising:

receiving, at the personal identification device, the travel permission information; and

sending from the personal identification device to a kill switch operatively coupled to the vehicle the travel permission information such that the kill switch disables operation of the vehicle when the travel permission information is invalid.

47.   (New) The processor-readable medium of claim 21, wherein the biometric input of the user is a first biometric input of the user, the user is an operator of a vehicle, the method further comprising:

receiving, at the personal identification device, the travel permission information; and

authenticating, at the personal identification device, a second biometric input from the operator based on the biometric template; and

sending from the personal identification device to at least one of a trucking company or a travel-governing institution via a transponder coupled to the vehicle the travel permission information when the second biometric input is authentic such that an identity of the operator is verified.

48.   (New) The processor-readable medium of claim 21, wherein the biometric input from the user is a first biometric input from the user, the user is an operator of a vehicle, the method further comprising:

receiving, at the personal identification device, the travel permission information;

authenticating, at the personal identification device, a second biometric input from the operator based on the biometric template; and

sending from the personal identification device to a kill switch operatively coupled to the vehicle the travel permission information to the kill switch when the second biometric input of the operator is authentic.

49.   (New) The processor-readable medium of claim 21, wherein the biometric template is stored only at the personal identification device.

50.   (New) The processor-readable medium of claim 21, wherein the personal identification device is configured to prevent output of the biometric template.

51.   (New) The processor-readable medium of claim 29, wherein the user is an operator of a vehicle, the processor device being associated with a remote party, the method further comprising:

sending a kill signal from the processor device to a kill switch operatively coupled to the vehicle such that the kill switch disables operation of the vehicle when the travel permission information is invalid.